CIBERDELINCUENCIA UNA REALIDAD - VIRTUAL CONTADA A MEDIAS

Reyes Neira Juan Manuel
Juanmanuelreys84@hotmail.com
Universidad Piloto de Colombia
Bogotá D.C - Colombia

Resumen— Las personas en su gran mayoría conocen los riesgos de seguridad con los que se debe convivir a diario, y que están latentes en diversos lugares que se frecuentan tales como: centros comerciales, bancos, el supermercado, la oficina, incluso en el hogar. Lo interesante es que los seres humanos con el paso del tiempo desarrollan una serie de habilidades que muchas veces en conjunto con diversas actividades, logran que estos riesgos se reduzcan de manera significativa, dando así tranquilidad en el momento de sortear cualquier eventualidad asociada a los mismos, demostrando que los seres humanos crean una serie de patrones de comportamiento preventivo que al final de cuentas se traduce en seguridad.

Ahora bien, de lo anterior podemos deducir que esos patrones sólo son aplicados, en la mayoría de los casos en el mundo real, dejando de lado lo que pasa en ese mundo virtual llamado internet, el cual ha evolucionado de forma tal que casi todo lo que podemos imaginar en nuestro mundo real se conseguirá en la WWW, y que al final de cuentas puede ser tan o más real que el mundo en el que vivimos a diario.

Por lo anterior, en este artículo se pretende plasmar de forma clara qué es la ciberdelincuencia, los riesgos que esta conlleva, su posible afectación, y cómo combatirla.

Abstract— People mostly known security risks with which they must live daily, and which are latent in many places you frequent such as shopping centers, banks, supermarket, office, even at home. The interesting thing is that human beings over time develop a range of skills that often in conjunction with various activities, manage these risks are reduced significantly, thus giving tranquility upon circumvent any eventuality associated with them, demonstrating that human beings create a series of preventive behavior patterns that in the end translates into safety.

But of this we can deduce that these patterns are only applied, in most cases, in the real world, ignoring completely what is happening in the virtual world called the internet, which has evolved in a way that almost everything you can imagine in our real world will be achieved in the WWW, and that in the end may be as or more real than the world in which we live every day.

Therefore, this article intends to translate clearly that is the cyber-crime, the risks that this entails, as well as their possible involvement, and to know how to fight.

Palabras Clave— Ataques DDoS, Ataques de denegación de servicio, Ciberacoso, Desfalcos financieros,Phishing, PWC (PricewaterhouseCoopers), Software Malicioso, Spammers, Suplantación de identidad, Virus informático.

I. INTRODUCCIÓN

La tecnología evoluciona a pasos agigantados acompañada siempre de los riesgos inherentes de ese proceso de desarrollo que se denota acelerado, en donde siempre se tendrá en el medio la información, la cual es el activo más importante e invaluable con el que cuentan las personas. En muchos casos se olvida el papel relevante que la información juega en el mundo de la WWW, y cómo su evolución beneficia de manera directa a las personas que realmente necesitan los servicios prestados por esa tecnología de avanzada, y también, a aquellas que sólo buscan utilizarla para hacer daño y obtener beneficios propios

infringiendo las leyes y violentando cuanto sistema informático encuentren en su camino, logrando de esta manera obtener esa recompensa anhelada llamada información.

En este artículo ahondaremos en lo que se denomina ciberdelincuencia, su impacto, sus riesgos, y cómo evitar los mismos para no ser engañados y caer en fraudes.

II. CIBERDELINCUENCIA

La ciberdelincuencia se define con carácter general como cualquier tipo de actividad ilegal en la que se utilice internet, una red privada o pública o un sistema informático doméstico.

Aunque muchas formas de ciberdelincuencia giran en torno a la obtención de información sensible para usos no autorizados, otro ejemplo es la invasión de la intimidad del mayor número posible de usuarios de ordenadores.

La ciberdelincuencia comprende cualquier acto criminal que utilizase ordenadores y redes. Además, la ciberdelincuencia también incluye delitos tradicionales realizados a través de internet. Por ejemplo: los delitos motivados por prejuicios, el tele mercadeo y fraude de internet, la suplantación de identidad y el robo de cuentas de tarjetas de crédito se consideran ciberdelitos cuando las actividades ilegales se llevan a cabo utilizando un ordenador e internet.[1]

Algunos de los ataques de los Ciberdelincuentes más comunes son:

- **Phishing:** El "phishing" consiste en el envío de correos electrónicos que aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario, que posteriormente son utilizados para la realización de algún tipo de fraude.

  Para ello, suelen incluir un enlace que, al ser pulsado, lleva a páginas web falsas. De esta manera, el usuario, creyendo estar en un sitio de confianza, introduce la información solicitada, que en realidad, va a parar a manos del estafador. [2]

  Los principales daños provocados por el phishing son:

  - **Robo de identidad y datos** confidenciales de los usuarios. Esto puede conllevar pérdidas económicas para los usuarios o incluso impedirles el acceso a sus propias cuentas.
  - **Pérdida de productividad.**
  - **Consumo de recursos de las redes** corporativas (ancho de banda, saturación del correo, etc.). [2]

Imagen 1
Ejemplo de phishing

Tomada de
http://www.pandasecurity.com/colombia/homeusers/security-info/cybercrime/phishing/.

- **Malware:** Es la abreviatura de "Malicious software", término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar términos como: Virus, Troyanos, Gusanos, espías de teclado, Botnets, Ransomwares, Spyware, Adware, Hijackers, Keyloggers, FakeAVs, Rootkits, Bootkits, Rogues, etc.[3]

- **Ataques de denegación de servicio DDOS:** es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la

víctima o sobrecarga de los recursos computacionales del sistema de la víctima.[4]

- **Ciberacoso:** El ciberacoso o ciberbullying es el acoso o la intimidación en internet. Puede producirse a través de un email, mensaje de texto, en un juego, o en un sitio de redes sociales. Esta práctica podría involucrar circular rumores o imágenes subidas al perfil de alguna persona o circuladas para que otros las vean, o crear un grupo o página para excluir a una persona.[5]

- **Suplantación de identidad:** es un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El cibercriminal, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas. [6]

- **Desfalcos financieros:** El desfalco o malversación es el acto en el que uno o más individuos se apropian indebidamente de valores o fondos que les han sido confiados en razón de un cargo. Es un tipo de fraude financiero. Puede referirse tanto a caudales privados, como públicos. Para este caso nos centraremos en los que se realizan utilizando medios electrónicos. [7]

III. EL IMPACTO DE LA CIBERDELINCUENCIA

¿Qué tan cuidadoso es usted con la información que comparte en las redes sociales, correo electrónico, herramientas de almacenamiento en la nube, dispositivos electrónicos?, ¿sabe usted quién está detrás del manejo de esta información?, ¿conoce los acuerdos de confidencialidad que acepta cuando se convierte en miembro de estas redes sociales?, ¿es seguro su computador?, ¿qué nivel de sensación positiva de seguridad tiene usted frente a los demás?, ¿por ser una pequeña empresa cree que está exento de un ataque?, ¿sabe cuánto valen las fotos de vacaciones en la playa?

¡CUIDADO!, USTED TAMBIÉN PUEDE SER VICTIMA.

Se estará preguntando acerca de estas pocas indagaciones de las tantas que pudiésemos llegar a realizar. Realmente mi estimado lector, se plasman con el ánimo de ponerlo a pensar un poco, en qué pasaría si su información fuese hurtada, si sus cuentas bancarias fuesen vaciadas, si llegase a encontrar las fotos del paseo de playa de fin de año de su familia, editadas y publicadas en páginas de pornografía. ¿Cree que usted está a salvo de estos posibles eventos? Finalmente usted lector es quién tiene la respuesta.

A menudo empresarios, profesores, deportistas, bomberos, policías y muchas más personas siente que nunca les tocará estar involucrados en un caso de ciberdelincuencia, pero desafortunadamente, para los ciberdelincuentes no existen objetivos pequeños, no existen victimas pequeñas, ellos sólo quieren lograr su objetivo a toda costa.

Es preocupante ver cómo la gente ignora lo que pasa a su alrededor, afortunadamente muchos cuentan con suerte y otros con el conocimiento, lo que no quiere decir que nunca les pueda pasar. Es preocupante ver cómo con el paso del tiempo la ciberdelincuencia crece, se estructura cada vez es mejor y más fuerte, mientras que las personas y los empresarios se quedan esperando a que no les pase, y este comportamiento se presenta porque no logran dimensionar el impacto que podría generar un ataque de ciberdelincuencia sobre sus empresas, o incluso, sobre su propia vida personal.

A. Impacto de los crímenes económicos

La delincuencia económica se presenta en muchas variedades, cada una con sus propias características, amenazas y consecuencias estratégicas.

Los delitos económicos siguen siendo una preocupación importante para las organizaciones de todos los tamaños, en todas las regiones y prácticamente en todos los sectores. Uno de cada

tres informes de las organizaciones muestra que son golpeadas por los delitos económicos.

1. Tasas de fraudes reportados

A continuación se muestran las estadísticas de crímenes económicos de 2001 a 2014 a nivel mundial.

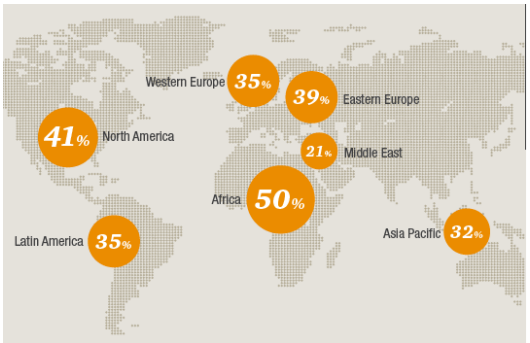
Imagen 2
Reporte global de fraudes

Tomada de
http://www.pwc.com/gx/en/economic-crime-survey/[8]

2. Dónde ocurre el crimen económico

Ningún continente está exento de esta amenaza pero gracias al estudio de la PWC (Price WaterhouseCoopers LLP) podemos identificar los porcentajes de estos ataques a nivel mundial, en el estudio es posible identificar que el continente africano es el más afectado por este tipo de ataques, seguido de los Estados Unidos.

Imagen 3
Porcentaje de ocurrencia de crímenes económicos



Tomada de
http://www.pwc.com/gx/en/economic-crime-survey/ [8]

3. El impacto económico

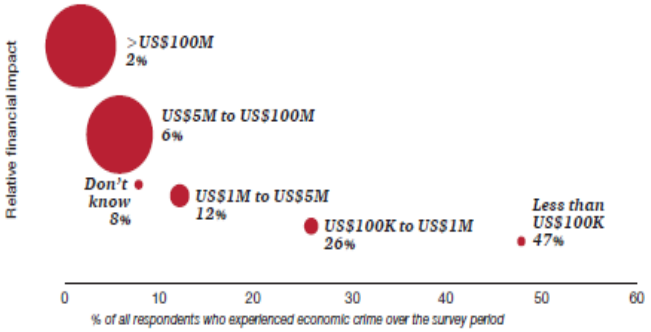
Las organizaciones a menudo no comprenden el verdadero impacto financiero de un delito económico hasta después de que ha ocurrido, a veces, mucho después. [9]

Aproximadamente una de cada cinco (18%) de las organizaciones que sufren crímenes financieros han experimentado un impacto financiero entre US $ 1 millón y US $ 100 millones. Y el porcentaje de empresarios que informaron pérdidas de más de US $ 100 millones se duplicó, de uno a dos por ciento en el transcurso de tres años.

Mientras que la categoría de más de US $ 100 millones es relativamente pequeño, lo que representa 30 organizaciones aproximadamente a nivel mundial, es de tener en cuenta que las cifras van en aumento y se arraigan como los principales impactos negativos de fraudes sistémicos a nivel corporativo.

Estas grandes pérdidas pueden ser alineadas con el aumento reportado en los casos de soborno y corrupción que puede ser especialmente costoso para las organizaciones, con multas reglamentarias, honorarios legales y gastos de remediación que potencialmente llegan a miles de millones de dólares y se podría decir que son los daños colaterales del cibercrimen. [9]

Imagen 4
Porcentaje de pérdidas a nivel mundial



Tomada de
http://www.pwc.com/gx/en/economic-crime-survey/cybercrime.jhtml[8]

B. Impacto social de la ciberdelincuencia

Se podría pensar que el impacto social del cibercrimen no es tan relevante por ser simplemente un tema de la www o internet, ese mundo virtual en donde, como su nombre lo indica, todo es aparentemente intangible. Pero realmente es tan o más sensible que el impacto generado por la delincuencia real.

Si bien el acceso a internet y el comercio electrónico han crecido exponencialmente en los últimos años, también se han incrementado los delitos informáticos.

Así lo confirmó el vice fiscal Jorge Fernando Perdomo, quien reveló que "en 2014 se realizaron más de 800 investigaciones en las que fueron utilizados medios informáticos para la comisión de delitos contra la información y los datos contra el patrimonio, la administración pública, el orden económico y social".

Agregó que "inicialmente se ha hecho una radiografía nacional y de criminalidad, y esto no se había hecho aquí en la Fiscalía hasta el año pasado. Con esto hemos identificado tres tipos de modalidad con gran impacto económico y social: Hurto por medio informático, accesos abusivos a sistemas informáticos que permiten la interceptación ilícita de comunicaciones y por último los señalamientos de injuria y calumnia que se hacen por medios informáticos".

Así las cosas, se descubrieron 159 casos por violación a la protección de la información y los datos; 124 hechos contra la administración pública; 101 por afectaciones a la libertad individual; 80 por patrimonio económico; 73 por seguridad pública; 70 por delitos contra el orden económico y social.

25 hechos que atentaron contra la vida y la integridad personal; 12 por conductas contra personas y bienes protegidos por el derecho internacional humanitario; 34 por afectaciones a la libertad, integridad y formación sexual; 21 contra la integridad moral y 16 por atentados a los derechos de autor.

El resto de investigaciones se adelantan por delitos contra la fe pública; los recursos naturales y el medio ambiente; la salud pública; la participación democrática; la eficaz y recta impartición de justicia; y el régimen constitucional y legal.

Por su parte, Jorge Silva, presidente de Microsoft Colombia, alertó que "el cibercrimen aumenta cada año un 50% por lo que más de un millón de personas están siendo afectadas por estos delitos y llevándolo a un más allá, cada segundo doce personas se ven afectadas por este delito".

Y es que de acuerdo con el Reporte anual de Norton de 2013, más de 400 millones de personas son víctimas del cibercrimen en el mundo, lo que genera pérdidas por 113 billones de dólares, incluso un estudio del IDC de ese mismo año estimó que los usuarios gastaron 22 billones de dólares y por lo menos 1.5 billones de horas solucionando problemas de seguridad relacionados con software falsificado. [10]

Así es, estimado lector, las cifras son tan alarmantes que muchas de las personas afectadas han sufrido impactos y consecuencias tan severas que hoy día están pasando por situaciones muy delicadas de las cuales esperamos se tome la experiencia para no caer en ellas.

IV. RIEGOS DE LA CIBERDELINCUENCIA

La tecnología avanza rápidamente y su desarrollo innovador trae consigo muchas ventajas y nuevas tecnologías, las cuales traen de la mano los riesgos inherentes a las mismas en donde en la mayoría de la ocasiones no estamos preparados y se omiten, porque al parecer estos riesgos no parecen tener un impacto mayor, lo cual puede llegar a ser tan falso como esa misma sensación de seguridad que las personas creen tener a su favor.

Por eso mismo, mi estimado lector, la responsabilidad de tener comportamientos preventivos y seguros frente a las nuevas tecnologías no es sólo de los grandes o pequeños empresarios, es un tema de todos, dado que esos riesgos llegan también a los hogares y desafortunadamente en este punto, es donde la protección para mitigar los mismos es la más débil.

Algunos profesionales del riesgo piensan que la ciberdelincuencia es relevante únicamente para las personas técnicas y que debería ser abordado por

los departamentos de TI. Pero la ciberdelincuencia representa un riesgo significativo para las organizaciones porque afecta su habilidad para alcanzar objetivos estratégicos y operativos. Desafortunadamente, muchos negocios no saben lo que significa la ciberdelincuencia, la probabilidad de que sean afectados, la extensión de su impacto, y cómo gestionarlo mejor.

La ciberdelincuencia puede afectar a una organización de muchas formas diferentes, incluyendo:

a) Robo o fraude en línea
b) Robo de identidad
c) Extorsión
d) Robo de datos de cliente
e) Robo de propiedad intelectual
f) Espionaje industrial

La exposición a la ciberdelincuencia está relacionada con el nivel de actividades "on-line" llevadas a cabo por una organización, incluyendo el alcance de su presencia "on-line", el grado en que activos valiosos e información son almacenados "on-line", la fortaleza de la seguridad "on-line", y el grado de concienciación del riesgo en la cultura organizativa.

Para gestionar el riesgo de la ciberdelincuencia, debemos primero identificar el nivel de nuestras actividades "on-line", y determinar qué activos y actividades podrían ser afectados. Entonces podemos empezar a identificar, evaluar y gestionar nuestros ciberriesgos.

Los pasos siguientes serán de ayuda:

- **Entender y definir claramente los objetivos organizativos para las actividades "on-line"**. Reconocer los entornos diferentes y específicos "on-line" de nuestros interesados, y evaluar sus apetitos de riesgo.

- **Direccionar factores tanto culturales como técnicos**. Estos incluyen barreras culturales, dificultades en la comunicación, y los efectos de los prejuicios en las percepciones del ciberriesgo.

- **Reconocer las amenazas del ciberdelito tanto internas como externas**. Las amenazas internas pueden surgir de los errores de los empleados, de la pérdida accidental de datos, o de filtraciones maliciosas de datos corporativos confidenciales. Las amenazas externas podrían venir de piratas informáticos, grupos de presión, competidores o incluso gobiernos extranjeros hostiles, así como virus, infiltraciones, troyanos etc.

- **Establecer responsabilidad, control e incentivos para direccionar ciberriesgos**. Todo el personal senior debería de ser responsable de gestionar el riesgo cibernético en su área de responsabilidad, y deberíamos desafiar a los interesados que "no lo ven como su problema".

- **Gestionar los ciberriesgos dentro del marco (ERM).** Los ciberriesgos pueden afectar a la empresa entera en áreas tales como la reputación, la continuidad del negocio y el efecto "edad" de las delegaciones y suministradores, de forma que necesite enfrentarse de una forma coherente como parte de nuestra respuesta global al riesgo.

- **Desarrollar una perspectiva global del impacto del riesgo de los delitos informáticos.** Muchas organizaciones dependen de la economía del extranjero para el comercio, las exportaciones y la generación de salud, y esto les expone a los delitos informáticos en el extranjero que no se pueden ignorar.

  Entendiendo los riesgos a los que se están expuestos, se debe incluir la ciberdelincuencia en nuestro pensamiento y práctica, de forma que podamos ofrecer un consejo práctico a nuestras organizaciones y hogares con el fin de reducir la amenaza y proteger nuestro negocio. [11]

Cuide su información es el activo más preciado con el que cuenta, sea precavido con las publicaciones que realiza de la misma y mitigue de esta forma la posibilidad de ser víctima de la ciberdelincuencia.

V. CÓMO HACERLE FRENTE A LA CIBERDELINCUENCIA

Es bueno que todos tanto empresarios, empleados, padres de familia, y demás desarrollen hábitos seguros para así poder estar preparados para poder enfrentar la ciberdelincuencia de manera segura.

Con el paso del tiempo y a medida que una persona crece va conociendo los riesgos que existen en su vida, su ciudad, su vecindario y demás para que de manera casi que implícita y apoyados de la experiencia de otros empiecen a crear comportamientos seguros y hábitos que ayudan a combatir que la delincuencia llegue de la manera más fácil a sus vidas, lo mismo se quiere lograr estimado lector frente a la ciberdelincuencia y esperamos que con las recomendaciones que a continuación se exponen logre que su conocimiento y prevención este más arraigada a la protección de usted mismo y la de los demás.

1. No herede sus datos a desconocidos:

Una de las maneras más comunes e "inocentes" de perder información sensible es el traspaso o rotación de dispositivos, sean personales o corporativos. Esto incluye equipos de cómputo, celulares y USB. "El sistema operativo de una computadora, dispositivo móvil o disco extraíble funciona de tal manera que cuando se borra un archivo, éste no desaparece físicamente, sino que en muchas ocasiones se almacena en un espacio de la memoria donde permanecerá por si se decide recuperarlo".

Así pues, al regalar o vender un celular usado, cambiar de equipos de cómputo, o prestar su memoria USB, sus datos sensibles pueden estar en peligro; aún tras formatearlos, éstos pueden ser recuperados por gente con cierta destreza.

"Si al dejar nuestros equipos o discos extraíbles no tenemos cuidado de realizar una limpieza segura para borrar toda la información, se corre el riesgo que ésta caiga en manos no deseadas".[12]

2. Usar contraseñas y cifrado a diario:

Las personas olvidan lo que llevan en el dispositivo, y cuando son víctimas de un robo es cuando se dan cuenta de todo lo que puede quedar comprometido con la información que cargaban. Por eso, lo primero que se debe hacer es poner una contraseña al disco extraíble utilizado, a sus dispositivos electrónicos y computadores portátiles si es posible, habilitar una opción para que se pueda borrar la información de manera remota.

3. No olvidar que está manejando información sensible:

La primera cosa que se debe recordar siempre, es la importancia que tiene la información sensible. A nivel personal, esto requiere tomar conciencia de los datos que se tiene en las manos para aprender a cuidarlos mejor y no dejar el celular o la memoria sobre la mesa del restaurante o el cibercafé al alcance de cualquiera.

En el ámbito corporativo se requiere la implantación de políticas de seguridad de la información para todos los empleados.

Como referencia, según el Reporte de Cibercrimen de Norton de Symantec, se estima que sólo en Colombia más de 9,7 millones de personas han sido víctimas de delitos informáticos en los últimos doce meses, y que estos delitos generaron pérdidas financieras directas por un monto de $79.180 millones de pesos.

No olvide también:

- Las redes sociales están en la mira de los Ciberdelincuentes.

- No usar la misma contraseña para todo. [12]

4. Links de Correo Electrónico:

Tenga cuidado cuando responda correos electrónico que no sean fiables para usted y más aún cuando quiera revisar los enlaces incorporados en estos mensajes.
Antes de hacer clic en algún enlace de mensajes de correo electrónico o en sitios web, comprobar que la dirección se va a un sitio bien establecido.

5. Amigo empresario aplique la Ciberresiliencia

La ciberresiliencia se trata de la administración de riesgos, no de su eliminación. La eliminación no solo es imposible, sino que impide la agilidad; un entorno con un nivel aceptable de riesgo admite innovación.

Implemente la estrategia de seguridad correcta ahora mismo.

El conocimiento es poder: las organizaciones ciberresilientes reconocen que las necesidades de seguridad van más allá de los sistemas, el software o los departamentos de TI, e implican un mayor conocimiento sobre seguridad por parte de todos los empleados y mejores procesos organizativos. Symantec propone una nueva asociación estratégica entre la función de seguridad y los líderes empresariales para equilibrar la ventaja competitiva y los ciberriesgos ineludibles de la actualidad y, de esta manera, lograr ciberresiliencia sin necesidad de estar libre de ciberriesgos.

Tome conciencia de su nivel de seguridad y conozca qué problemas de seguridad son más importantes para su organización.
Utilice este conocimiento para mantener a sus colegas al tanto de las prácticas recomendadas.
Cree una estrategia de seguridad que equilibre la ventaja competitiva con el ciberriesgo continuo y desconocido. [13]

VI. CONCLUSIONES

Después de leer el artículo y conocer de una manera breve el impacto que genera la ciberdelincuencia a nivel mundial, es prudente estimado lector que usted desde ya, aplique todas las acciones preventivas que estén a su alcance frente a estos incidentes. No espere a que le pase ya que como se pudo dar cuenta los impactos pueden llegar a ser catastróficos, no se fie de ese mundo virtual que parece inofensivo, pero que en realidad puede llegar a ser tan o más real que el mundo en el que vivimos. Advierta a su familia, amigos y conocidos sobre este tema, no permita que ellos continúen dejándole al azar la seguridad en la internet.
Siempre este alerta y vigilante frente a cualquier sospecha que tenga cuando realice transacciones electrónicas, si es necesario cancélelas, use herramienta de protección como antivirus pagas, e informe a las autoridades de inmediato en caso de que se viera involucrado en un incidente de este estilo.

REFERENCIAS

[1] BullGuard Security Centre
http://www.bullguard.com/es/bullguard-security-center/internet-security/security-tips/cybercrime.aspx
[2] Panda Security
http://www.pandasecurity.com/colombia/homeusers/security-info/cybercrime/phishing/
[3] Info Spyware
https://www.infospyware.com/articulos/que-son-los-malwares/
[4] Wikipedia
https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio
[5] Alertaenlinea.gov
https://www.alertaenlinea.gov/articulos/s0028-ciberacoso
[6] Wikipedia
https://es.wikipedia.org/wiki/Phishing
[7] Wikipedia
https://es.wikipedia.org/wiki/Desfalco
[8] PWC
http://www.pwc.com/gx/en/economic-crime-survey/
[9] PWC
http://www.pwc.com/gx/en/economic-crime-survey/cybercrime.jhtml
[10] Vanguardia
http://www.vanguardia.com/colombia/300961-un-millon-de-personas-afectadas-por-el-cibercrimen-microsoft
[11] PMI Ben Rendle
http://www.pmi-mad.org/index.php?option=com_content&view=article&id=771:grcd&catid=137:articulos&Itemid=88N
[12] wradio
http://www.wradio.com.co/noticias/sociedad/ojo-con-la-informacion-de-sus-celulares-consejos-para-enfrentar-la-ciberdelincuencia/20130204/nota/1836186.aspx
[13] Symantec
http://www.symantec.com/es/mx/page.jsp?id=cyber-resilience